Annual Privacy Act Training & Safeguarding Personally Identifiable Information

Washington Headquarters Services
Executive Services Directorate
Office of Freedom of Information

Why You Are Being Asked to Take this Training Now

- The Office of Management and Budget, the Federal entity responsible for overseeing the Privacy Act, has mandated that the Federal workforce and contractors accessing and using PII in the course of a government contract complete this training.
- Since May 2006, there have been a number of instances where personal data has been lost, stolen, or compromised. The most publicized incident occurred when a Federal employee took home data on 26.5 million veterans in violation of Department of Veterans Affairs policy, and the laptop was stolen.
- Don't YOU or a member of your staff be the next accused of carelessly handling personal data!

Overview of the Privacy Act of 1974

Main Points

- Statutory/Regulatory Authority
- Purpose of the Act
- Information Protected by the Act
- Primary Features of the Act
- Disclosure
- System of Record Notice
- Privacy Act Statement
- Social Security Number Solicitation
- Individual Request for Record
- Safeguarding Privacy Act Information
- Criminal and Civil Penalties
- Your Role and Responsibility
- Contact Information

Overview of the Privacy Act of 1974

Statutory/Regulatory Authority

- Statutory authority.
  - The Privacy Act of 1974, as amended (5 U.S.C. 552a), as implemented by OMB Circular No. A-130
- DoD Regulatory authority:
  - DoD Directive 5400.11
  - DoD Regulation 5400.11-R
  - OSD Administrative Instruction No. 81

Purpose of the Act

- The Privacy Act of 1974 was enacted to safeguard individual privacy contained in Federal records and to provide individuals access and amendment rights to records concerning them which are maintained by Federal agencies.
- By establishing the Privacy Act, Congress intended to put in proper balance individual privacy with the Government's need to maintain information about individuals.

Overview of the Privacy Act of 1974

Information Protected by the Act

- Examples of records subject to the Privacy Act are any of the following:
  - Social Security Number
  - Home address
  - Home telephone number
  - Complete date of birth
  - Personal medical information
  - Personal/private information (required for security clearance or similar use)

- This type of data is knows as Privacy Data (in the Privacy world) or Personally Identifiable Information (PII) in the Information Assurance world)
- Whenever a Federal agency maintains information about individuals and retrieves it by a personal identifier, the collected records are a Privacy Act system of records.

Overview of the Privacy Act of 1974

Primary features of the Act

- Restricts disclosure of personal information from systems of records.
- Requires Federal agencies to comply with the law for collecting, maintaining, using, and disseminating information from personal records.
- Provides individuals with access to records about themselves.
- Allows individuals to request amendments to records which are inaccurate, irrelevant, untimely, and incomplete.
- Addresses the collection, maintenance use and dissemination of Social Security Numbers
- Provides legal remedies, both civil and criminal, for violations of the Privacy Act.

Overview of the Privacy Act of 1974

Privacy Definitions

- Individual – A living person who is a citizen of the U.S. or an alien lawfully admitted for permanent residence.
  - Not included in coverage are records agencies might maintain on non-U.S. citizens who are not aliens admitted for permanent residence, organizations and businesses, including small businesses, even where the company's trade name is the same as that of the owner.
  - For deceased persons, the release of information is protected when release would invade the privacy of the surviving next of kin.
- Personally Identifiable Information– Information about an individual that identifies, relates or is unique to, or describes him or her; e.g., SSN, medical history, biometrics, date of birth, home address/telephone number.
- Record - Any item, collection, or grouping of information, whatever the storage media, about an individual that is maintained by a DoD Component.

Overview of the Privacy Act of 1974

Privacy Definitions (cont.)

- Routine Use - Release of information outside the agency for a purpose compatible with the purpose for which the information was collected. Releases of information between DoD Agencies (i.e., Army to Navy or any other Defense Department Component) are not considered routine uses. However, Army to Department of Health and Human Services would be a routine use.

- System of records - A group of records under the control of a DoD Component from which personal information is retrieved by the individual's name or by some identifying number, symbol or other identifier assigned to the individual.

Overview of the Privacy Act of 1974

Disclosure

- No agency shall disclose any record which is contained in a system of records by any means of communication to any person or another agency without a written request or prior written consent of the individual to whom the record pertains unless the release has been established by a routine use.

- Disclosure includes any means of communication -- oral, written, or electronic.

- Disclosure does not occur if the communication is to those who already know.

Overview of the Privacy Act of 1974

System of Record Notice (SORN)

- Advance public notice must be given before an Executive Agency begins to collect personal information for a new system of records. This is done by publication in the Federal Register to provide an opportunity for interested persons to comment.

Privacy Act Statement

- The Privacy Act requires that, when an agency solicits information from an individual for a system of records, it must tell the individual in writing:
  - The statute or executive order of the President that authorizes the agency to solicit the information;
  - The principal purposes for which the information is intended to be used;
  - The routine uses which may be made of the information as published in the SORN in the Federal Register; and
  - Whether the disclosure of the information is mandatory or voluntary; and the effects, if any, on the individual for not providing the information.

Overview of the Privacy Act of 1974

Social Security Number Solicitation

- Section 7 of the Privacy Act makes it unlawful to deny any benefit, right, or privilege provided by law because the individual refuses to disclose his or her Social Security Number.

- Also, any time a SSN is asked for regardless of whether or not it is to be kept in a system of records, a Privacy Act Statement must be given.

- USD (P & R) Memo, March 28, 2008, “DoD Social Security Number (SSN) Reduction Plan” establishes the DoD policy in the use of the SSN and guidance for reducing its unnecessary use.

Overview of the Privacy Act of 1974

Individual Request for Record

- The individual about whom the record pertains is usually entitled to access his or her own record. The Privacy Act SORN for the pertinent records provides the address one may use to request access to his or her records. An agency must be prepared to grant access to the individual in person or by mail.
- With respect to personnel or any other Privacy Act system of records, if the individual believes information is in error, he or she should follow procedures in the system notice for requesting correction of the record. If the system manager refuses to make corrections requested by the individual, the individual may continue to pursue correcting his or her record through the appeal process.

Safeguarding Personally Identifiable Information

What is Personally Identifiable Information (PII)

Personally Identifiable Information is any information about an individual maintained by an agency, including, but not limited to the following:

- **Their name;**
- **Social security number;**
- **Date and place of birth;**
- **Mother's maiden name;**
- **Biometric records, etc., including any other personal information which is linked or linkable to an individual;**
- **Education;**
- **Financial transactions;**
- **Medical history;**
- **Criminal or employment history and information which can be used to distinguish or trace an individual's identity.**

Safeguarding Personally Identifiable Information

Safeguarding PII (Privacy Identifiable Information a.k.a Privacy Act Information)

- PII must always be treated as “FOR OFFICIAL USE ONLY” and must be marked accordingly. This applies not only to conventional records but also to electronic (including email) transmissions and faxes, which must contain the cautionary marking “FOUO” before the beginning of text containing Privacy Act information.

- When emailing PII, emails must be encrypted.

- PII records should be stored in filing cabinets or other containers so as to prevent unauthorized access.

Safeguarding Personally Identifiable Information

Storing PII

- **Duty Hours**
  - Cover or place in an out-of-sight location when those not authorized access enter the work space.
  - Use filtering devices on computer screens to blacken the view.
  - Lock computers when leaving – even for brief periods.
- **After Duty Hours**
  - If the building is locked or manned by security, place records in locked or unlocked drawer or cabinet.
  - Special Categories of Privacy data should be placed in locked receptacles.

- **What are Some Special Categories of PII?**
  - Investigative Files
  - Personnel Files
  - Security Clearance Files
  - Adverse Action Files
  - Any collection of PII that confers or deny a benefit to an individual

Safeguarding Personally Identifiable Information

Sharing PII

- Follow the "need-to-know" principle. Share only with those specific DoD employees who need the data to perform official, assigned duties.
- If the Privacy Act System Manager has granted you authority to make disclosures outside DoD:
  - Share only with those individuals and entities outside DoD that are listed in the "Routine Use" clause of the governing Privacy Act system notice.
- If you have doubts about sharing data, consult with your supervisor, the Privacy Act system manager, or your local Privacy Act Officer.

Safeguarding Personally Identifiable Information

Transporting PII

- Using E-mail:
  - Use Common Access Card procedures
  - Announce in the opening line of text that you are relaying FOUO material
  - Encrypt the e-mail before sending
- Handcarrying
  - Create a Cover Sheet stating “For Official Use Only” to shield contents.
- Using Ground Mail:
  - Use kraft or white envelopes.
  - You may double wrap using an inner and outer envelope if you deem it appropriate.
  - Mark the envelope to the attention of an authorized recipient.
  - Never use “holey joes” or messenger-type envelopes.
  - Never indicate on the outer envelope that it contains Privacy Data.

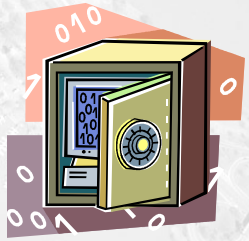
Safeguarding Personally Identifiable Information

Disposing of PII

- Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.
- Disposal methods <u>may</u> include:
  - Burning
  - Melting
  - Chemical decomposition
  - Pulping
  - Pulverizing
  - Shredding
  - Mutilation
  - Degaussing
  - Delete/Empty Recycle Bin

Safeguarding Personally Identifiable Information

Safeguarding Requirements

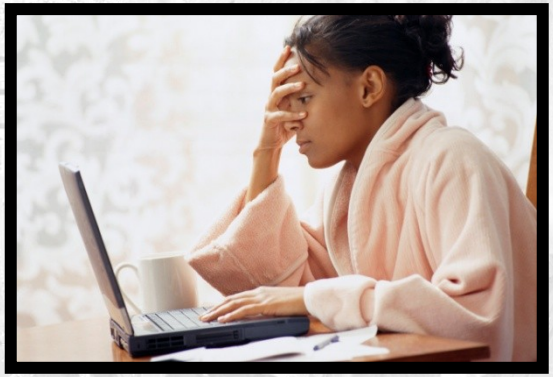


- Three Levels of Safeguards are Required:
  - Administrative
  - Physical
  - Technical
- These individuals are responsible for establishing safeguards:
  - Information Technology System Designers
  - Privacy Act System Managers
  - Local Privacy Act Officials
- These individuals are responsible for seeing that safeguards are applied:
  - YOU!

Safeguarding Personally Identifiable Information

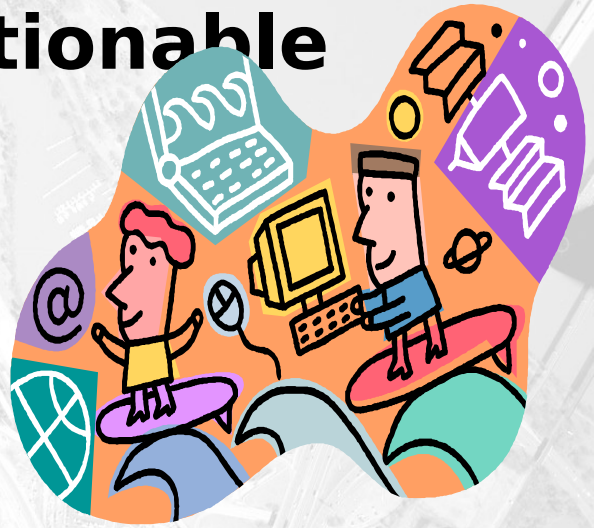
Information for Teleworkers

- **Paper Records:**
  - Place Privacy Act data in locked drawers, locked briefcases, or other secure areas where family or household members cannot access it
- **Electronic Records:**
  - Use password protection protocols. Share your password with no one.



Safeguarding Personally Identifiable Information

If You Find Something Questionable



- Immediately notify your supervisor, your local Privacy Act Officer, the Privacy Act System Manager, or any other appropriate official of the occurrence.
- For World Wide Web postings, make a note of where the information was posted by copying the Uniform Resource Locator (URL). The URL is the address listed at the top

Wrap Up

Criminal Penalties

- Any agency official or employee who willfully makes a disclosure of a record knowing it to be in violation of the Privacy Act or maintains a system of records without having published the requisite system notice may be convicted of a misdemeanor and fined up to $5000.
- Any person who knowingly and willfully requests or obtains a record of another individual from an agency under false pretenses may be convicted of a misdemeanor and fined up to $5000.

Wrap Up

Civil Penalties

- The Privacy Act also imposes civil penalties on violators who:
  - Unlawfully refuse to amend a record.
  - Unlawfully refuse to grant access to records
  - Fail to maintain accurate, relevant, timely and complete data
  - Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect.

- Penalties include:
  - Payment of actual damages
  - Payment of reasonable attorney's fees
  - Removal from employment

Wrap Up

If You Have Access to Personal Identifiable Information

- Protect it at all times.
- Do not share it with anyone unless
  - The recipient is listed in Section (b) of the Privacy Act or
  - The record subject has given you written permission to disclose it.
- Password protect personal data placed on shared drives, the Internet or the Intranet.
- Monitor your actions: If I do this, will I increase the risk of unauthorized access?

Remember:

You may be subject to civil and criminal penalties for violating the Privacy Act.

Wrap Up

Tips for Avoiding Privacy Breaches

- Take privacy protection seriously.
- Respect the privacy of others.
- Alert your supervisor or other management official when you see personal data left unattended.
- Know the Privacy Act requirements
- Ensure that all message traffic, faxes, and e-mails that contain personal information are properly marked and email is encrypted.
- Think Privacy before you seek to establish new data collections on your computer or similar office equipment.

Wrap Up

Your Role and Responsibility

- Do not collect Personally Identifiable Information without proper authorization
- Do not maintain illegal files; do not maintain or release inaccurate information
- Do not distribute or release personal information to individuals who do not have a need for access
- Do not maintain records longer than permitted
- Do not destroy records before records retention requirements are met
- Ensure that you do not place unauthorized documents in a records system
- Ensure that you mark all documents that contain privacy information “For Official Use Only – Privacy Act of 1974”; or “For Official Use Only – Privacy Act Data”.
- Ensure that all message traffic, faxes, and e-mails that contain personal information are properly marked and e-mail is encrypted.
- Think Privacy before you seek to establish new data collections on your computer or similar office equipment.

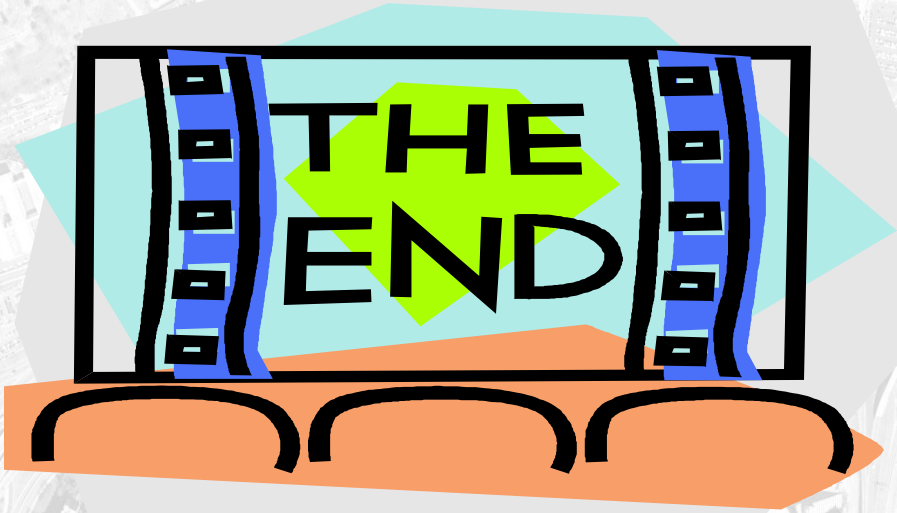
Questions or Concerns

Contact

- OSD/JS Privacy Office's website:
http://www.dod.mil/pubs/foi/privacy/

- Chief, OSD/JS Privacy Office:
Cindy Allard
(703) 588-6830
cindy.allard@whs.mil

You've just completed your Annual Privacy Act
&
Safeguarding Personally Identifiable Information Training



Thank you for completing this training!